OULUN SEUDUN
AMMATTIKORKEAKOULU

Sami Aho

6LOWPAN-IPV6-LIKIVERKKOJEN TIETOTURVA

6LOWPAN-IPV6-LIKIVERKKOJEN TIETOTURVA

Sami Aho
Opinnäytetyö
Syksy 2013
Tekniikan yksikkö
Tietotekniikan koulutusohjelma
Oulun seudun ammattikorkeakoulu

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Tietotekniikan koulutusohjelma, langaton elektroniikka

Tekijä(t): Sami Aho
Opinnäytetyön nimi: 6LoWPAN-IPv6-likiverkkojen tietoturva
Työn ohjaaja(t): Kari Jyrkkä
Työn valmistumislukukausi ja -vuosi: Syksy 2013
Sivumäärä: 32

Työn aiheena oli tutkia 6LoWPAN-protokollaan pohjautuvien järjestelmien tietoturvaa. Tavoitteena oli tuottaa dokumentti, jota voidaan hyödyntää langattomien järjestelmien opetuksessa ja pohjana tietoturvan ymmärtämiseksi.

Ensimmäisessä vaiheessa tutustuttiin IETF:n määrittelemiin Ipv6-likiverkkoja koskeviin standardeihin ja tietoturvaan liittyviin analyyseihin. Materiaalin perusteella kirjoitettiin tietoturvaan liittyvästä teoriasta ja mekaniikoista, joihin tietoturvariskit liittyvät.

Toisessa vaiheessa käytiin lävitse 6LoWPAN-järjestelmiin liittyviä tietoturvariskejä ja kerrottiin, millaisella tavalla näitä vastaan tulee suojautua ja kuinka turvallinen järjestelmä suunnitellaan. Tuloksena syntyi tämä dokumentti, jota voidaan käyttää 6LoWPAN-järjestelmien tietoturvariskien ja turvallisten järjestelmien suunnittelun aihetta opiskeltaessa.

Avainsanat:6LoWPAN, IPv6, likiverkko, sensoriverkko, tietoturva

ABSTRACT

Oulu University of Applied Sciences
Information Technology, Wireless Electronics

Author: Sami Aho
Title of thesis: 6LowPAN IPv6 Local Area Networks Information Security
Supervisor: Kari Jyrkkä
Term and year when the thesis was submitted: Fall 2013
Pages: 32

The basis of this work was to study the 6LoWPAN protocols information security and the systems based on 6LoWPAN & IEEE 802.15.4. The aim of the work was to produce a document that can be used in education and for the understanding of information security that applies these systems.

In the first phase the IPv6 network protocols defined by the IETF working group and other analytical studies about 6LoWPAN information security were studied. This documents first three topics was written on the basis of the material studied about the security mechanics and security risks associated with it.

The second phase of the work was to write about the security risks related to 6LoWPAN systems and how to design secure system. These topics are written in the documents later parts.

The result of this work was this document which can be used to teach and study the 6LoWPAN systems security risks and secure systems design.

Keywords: 6LoWPAN, IPv6, local area network, wireless sensor network,

TERMIT JA LYHENTEET

6LoWPAN	IPv6 matalan tehon likiverkko
Ad Hoc	Langattomien lähiverkkojen topologia
CIA	Confidentiality, integrity, availability. Tietoturvaperiaate; luottamuksellisuus, eheys, saatavuus
CGA	Cryptographically Generated Addresses, IPv6-osoitteiden salausmenetelmä
DAG	Directed Acyclic Graph, matemaattinen malli
DAD	Duplicate Address Detection, osoitteiden kaksoiskappaleiden tunnistusmekanismi
DODAG	Destination Oriented DAG, yksittäinen DAG-isäntä
DUD	Neighbor Unreachability Dedection, reitittimen tavoitukseen liittyvä mekanismi
HELLO flood	IP-pakettipohjainen palvelunestohyökkäys
IDS	Intrusion Detection System, tunkeilijan havaitsemisjärjestelmä
IPsec	IP Security Architecture, joukko TCP/IP-perheeseen kuuluvia tietoliikenne protokollia
IPv6	Internet Protokolla versio 6
OSI-malli	Open System Interconnection Reference Model, tiedonsiirtoprotokollien malli
ND	Neighbor Discovery, reitittimien yhdistykseen liittyvä mekaniikka
NS-viesti	Neighbor Solicitation, reitittimen pyyntöihin liittyvät viestit naapuri reitittimelle
NA-viesti	Neighbor Association, reitittimen yhdistymiseen liittyvät viestit naapurireitittimelle
NDP	Neighbor Discovery Protocol, viereisten reitittimien löytämiseen käytettävä protokolla
Nonce	Number once eli satunnaisluku, tiedon autentikointiin käytettävä luku
RD	Router Discovery, reititysmekanismi
RS-viesti	Router Solicitation, reitityspyyntöihin liittyvät viestit
RA-viesti	Router Association, reitittimien yhdistymiseen liittyvät viestit

SISÄLTÖ

1 JOHDANTO

Opinnäytetyön tutkimuksen kohteena ovat 6LoWPAN-standardin alaiset lyhyen kantaman tietoliikennejärjestelmät ja niiden tietoturva. Tutkimuksen tavoitteena on tutustua 6LoWPAN-tietoturvamekanismeihin ja luoda dokumentti, jota voidaan käyttää aiheeseen tutustumiseen.

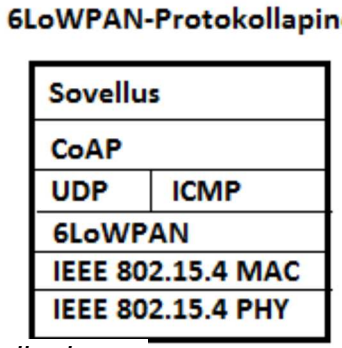
Tarkemmin tutkimuksessa käsitellään 6LoWPAN-standardin mukaisten järjestelmien tietoturvaa. 6LoWPAN-standardi mahdollistaa useiden laitteiden liittymisen Internettiin käyttäen IPv6-osoitteiston tuomaa osoitetilaa. 6LoWPAN-laitteita voidaan ohjata Internetin kautta ja ne voivat lähettää tietoa lähiverkon ulkopuolelle. Tutkimuksen tavoitteena on selvittää, miten 6LoWPANin tietoturva rakentuu ja minkälaisia mahdollisia tietoturva uhkia sen tulisi kestää. Tutkimuksessa käsitellään lisäksi, kuinka tietoturva-ominaisuudet vaikuttavat järjestelmän suunnitteluun. Motiivina tutkimukselle on lyhyen kantaman järjestelmien käytön yleistyminen teollisuudessa, kotiautomaatiossa ja kaupallisissa tuotteissa. Vahvan tietoturvan suunnittelu 6LoWPANia käyttävälle tuotteelle on haastavaa toteuttaa IPsec-tietoliikenneprotokollaa laitteiden heikon tehon takia.

Teoriaosassa käsitellään IETF:n (Internet Engineering Task Force) 6LoWPANiin liittyviä standardeja. Käydään lävitse 6LoWPANin ja 802.15.4-standardiin pohjautuvien järjestelmien rakennetta ja tietoturvaan liittyvää salausta tasoittain sekä niihin liittyvien turvauhkien periaatteita. Tutkitaan, kuinka tietoturva on toteutettu laitteistossa.

Toteutusosassa käydään lävitse järjestelmistä löytyneitä tietoturvauhkia ja sitä, kuinka järjestelmät suojautuvat näitä vastaan. Tulokset pohjautuvat 6LoWPAN-järjestelmiin toteutettuihin tietoturvatutkimuksiin.

2 6LOWPAN-JÄRJESTELMÄ

6LoWPAN-järjestelmät vaativat usein luotettavuus- ja yhtenäisyyssuojausta, jotka voidaan toteuttaa 6LoWPAN-protokollapinon (kuva 1) sovellus-, CoAP-, 6LoWPAN-, IEEE 802.15.4 MAC- ja PHY-tasoilla. Haasteena 6LoWPANissa on verkon vähäisten resurssien käyttö tietoturvaan. Erilaiset salaustekniikat ja tietoturva menetelmät vaativat järjestelmältä eri tavalla resursseja.



Kuva 1 6LoWPAN-protokollapino

2.1 6LoWPAN-verkon tietoturva

Langattoman 6LoWPAN-verkon tietoturvauhkia on tutkittu laajasti. 6LoWPANnin tietoturva vaatii erityyppisiä ratkaisuja riippuen hyökkäystavasta verkkoon. Verkon ulkopuoliset hyökkäykset voivat olla passiivia hyökkäyksiä, kuten salakuuntelua tai aktiivisia hyökkäyksiä. Aktiivisessa hyökkäyksissä verkkoon toteutetaan esimerkiksi palvelunestohyökkäys, jolloin verkon toimintaa estetään radiohäirinnällä tai pakettipohjaisella liikenteellä. 6LoWPAN-verkkoihin kohdistuvat tietoturvariskit kattavat protokollapinon jokaisen tason. (1; 2.)

6LoWPANin tietoturvamekanismit pohjautuvat yleisimmin tiedon salaukseen, jonka avulla verkon ulkopuolisia uhkia voidaan eliminoida. Tämä ei kuitenkaan auta tapauksissa, missä haavoittuvaisuus tai hyökkäys tapahtuu verkon sisäpuolelta. Verkon sisäpuoliset hyökkäykset voidaan toteuttaa kahdella eri periaatteella:

1 Hyökkääjä saa käsiinsä yhden verkon laitteista ja uudelleenohjelmoi laitteen.

2 Hyökkääjä käyttää ohjelmia ja laitteita, jotka murtavat verkon salauksen, tai injektoi verkkoon haittakoodia. (1; 2.)

Verkon sisäpuoliset hyökkäykset on tarkoitettu rampauttamaan verkon operointia tai verkon tietojen urkkimiseen. Tämän tyyppisten hyökkäyksien estämiseksi tulee kriittisissä 6LoWPAN-verkoissa käyttää verkkotoiminnan monitorointia, jonka avulla voidaan havaita verkon epänormaali käyttäytyminen. Mikäli tietoturvauhkaa ei havaita ajoissa verkossa, voi mahdollinen haitta olla erittäin vakava ja pitkäkestoinen. Tämän tyyppisiä hyökkäyksiä on esimerkiksi Sybil-hyökkäys, missä hyökkääjä käyttää paketin väärentämismekaniikkaa, joka johtaa erilaisiin uudelleenreititys- ja palvelunestohyökkäyksiin. Sinkhole-hyökkäys, missä hyökkääjä onnistuu ohjaamaan paketit määrättyyn laitteeseen. (1; 2.)

2.2 IEEE 802.15.4 -standardiin liittyvä tietoturva

IEEE 802.15.4 -standardi määrittelee lyhyen kantaman radioiden fyysisen ja MAC-kerroksen sekä perusteet sen alla olevien radioiden tietoturvaan. Standardi toimii seuraavien spesifikaatioiden pohjana: 6LoWPAN, Zigbee, ISA 100.11a, WirelessHART, jotka ovat määritelleet omien spesifikaatioiden mukaan ylemmät tasot sovelluksista ja niiden tietoturvan. (1; 3.)

802.15.4-standardi protokolla pohjautuu Internetin OSI-malliin siirtoyhteyskerroksen määrittelyihin RFC 1122 ja RFC 1123, joiden tietoturva-osioita on sovellettu matalatehoisiin lyhyen kantaman järjestelmiin sopiviksi. (1; 3.)

802.15.4-standardin nykyinen versio käsittää useita eri tietoturvaan liittyviä ominaisuuksia. Niiden käyttö mahdollistaa CIA-periaatteen mukaisen tietoturvan. CIA-periaate muodostuu tietoturvan luotettavuudesta, eheydestä ja saatavuudesta. Osassa tietoturvaominaisuuksista on kuitenkin havaittu haavoittuvuuksia ja niiden toiminta tulee huomioida järjestelmän tietoturvassa. (1; 2; 3.)

802.15.4-standardin tietoturvan on suunniteltu tukemaan useiden erilaisten järjestelmien toimintaa. Tietoturvan tulee kattaa esimerkiksi kohteen

turvallisuuteen liittyvät järjestelmät, kuten erilaiset hälyttimet kiinteistössä, tehtaiden mittausjärjestelmät ja ihmisten seuranta. Mikäli järjestelmä ei käytä mitään standardissa olevaa tieturvaominaisuutta, voi hyökkääjä muuttaa haitallisesti järjestelmän toimintaa. (1; 2; 3.)

Langattomien järjestelmien tietoturvan tulee osata hallita monia erityyppisiä hyökkäyksiä. Järjestelmiä vastaan voi hyökätä esimerkiksi erityyppisillä palvelunestohyökkäyksillä, salakuuntelulla ja fyysisesti vahingoittamalla järjestelmää. Palveluestohyökkäykset ovat tyypillisesti suuri tehoisia haitallisia lähetyksiä samalla taajuusalueella tai niin kutsuttua ”HELLO flood” -tyyppistä viestitystä järjestelmään, jolloin viestien välitys keskeytyy järjestelmässä. (1; 2; 3.)

3 6LOWPAN-LIKIVERKKOJEN TIETOTURVA

Tässä osiossa tutustutaan 6LoWPAN-järjestelmien reititykseen ja niihin liittyviin tietoturvamekanismeihin.

3.1 6LoWPAN-likiverkkojen reititys ja topologia RPL

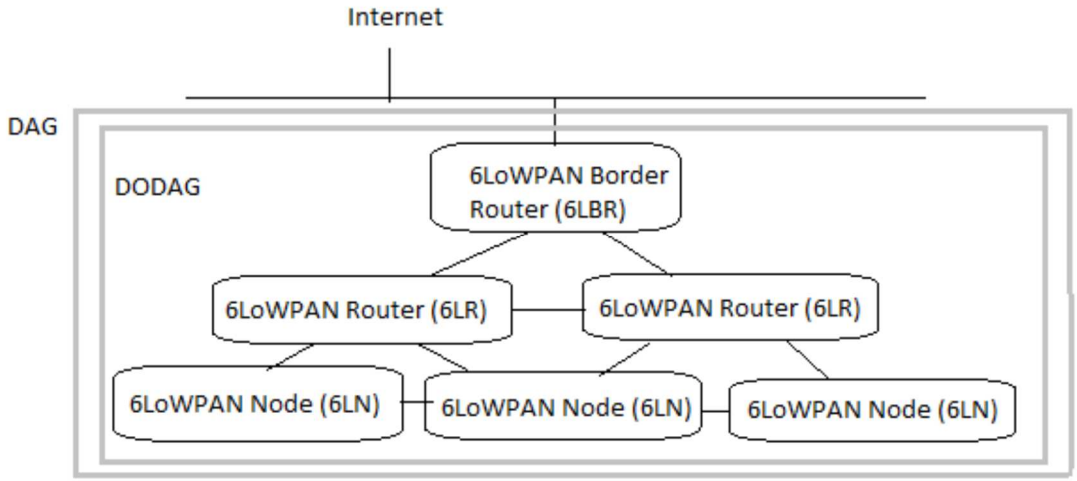
6LoWPAN-verkkojen reititysprotokolla on määritelty IETF:n standardissa RFC 6550, ja sen nimeksi on annettu RPL. Se suunniteltiin toimimaan ympäristössä, jossa verkon laitteiden väliset yhteydet ovat tyypillisesti rajoitettuja laitteiden vähäisen tehon, muistin ja virtalähteen käyttöiän takia. Tämän tyyppisten laitteiden tiedonsiirtoa haittaavat suuret datapakettien häviöt, hitaat tiedonsiirtoyhteydet ja epävakaudet.(7, s. 7–8.)

RPL tukee tiedonsiirtoa kahden verkon sisäisen laitteen välillä, keskeisen (yhdestä-yhteen), kontrolloivan reitittimen ja sen aliverkon laitteiden välillä (yhdestä-moneen*)* sekä aliverkon laitteiden ja verkkoa kontrolloivan reitittimen välillä (monesta-yhteen) (7, s. 7–9**).**

3.1.1 RPL:n osat

Reititysprotokollan (kuva 2) osat ovat seuraavat:

- 6LoWPAN Node (6LN): Aliverkon laite, joka toimii verkon reitittimenä tai isäntänä.
- 6LoWPAN Router (6LR): Paikallisen verkon reititin, joka voi lähettää RA-viestejä ja vastaanottaa RS-viestejä sekä välittää ja reitittää Ipv6-paketteja.
- 6LoWPAN Border Router (6LBR): Verkon reititin, joka sijaitsee paikallisen verkon reunalla. Reitittää erillisiä 6LoWPAN-verkkoja tai 6LoWPAN-verkon IP-verkkoon. (13, s. 9.)



Kuva 2. Reitityksperiaate

6LoWPAN-verkkojen laitteet muodostavat verkon käyttäen DAG (Directed Acyclic Graph) -periaatetta. DAG mahdollistaa verkon topologian (kuva 2) luonnin siten, että järjestelmien välisiin yhteyksiin ei muodostu silmukoita. DAG voidaan tämän jälkeen jakaa useiksi aliverkoiksi, joiden nimitykseen käytetään nimeä: Destination oriented DAG *(DODAG*). DODAG muodostuu verkon reunareitittimen 6LBR ja sen alaisista 6LR- ja 6LN -laitteista. (7, s. 9–14.)

3.1.2 RPL:n tunnisteet

RPL käyttää neljää eri tunnistetta topologian ylläpitämiseksi:

- RPLInstanceID: Verkolla voi olla useita RPLInstanceID-arvoja, jotka sisältävät sen alaisten DAG:iden tiedot. Tätä arvoa käytetään verkon topologian optimointiin.
- DODAGID: DODAGin tunnistearvo, käytetään yhdessä RPLInstanceID:n arvon kanssa jokaisen verkon laitteen tunnistamiseen.
- DODAGVersionNumber: DODAGin isännän numero. RPLInstanceID, DODAGID ja DODAGVersionNumber avulla tunnistetaan verkon uniikit aliverkot DODAGit.
- Rank: DODAGin alaisten laitteiden eli 6LR- ja 6LN-laitteiden asema verrattuna verkon isäntään DODAGVersionNumber. (7, s. 14.)

6LoWPAN-verkoilla ei tyypillisesti ole valmiiksi määriteltyä topologiaa, joten RPL:n on löydettävä laitteet ja määriteltävä optimaalisin reitti tarkkaan. Verkon topologian luonti aloitetaan tyypillisesti 6LBR-reititinlaitteesta. RPL jakaa verkon ensin yhteen tai useampaan DAG:iin, joiden tunnisteet lisätään RPLInstanceID-arvoon. DAG:n alle määritellään tämän jälkeen DODAGit eli aliverkot, jotka voidaan tunnistaa käyttämällä DODAGID ja RPLInstanceID-arvoja. DODAGit muodostuvat verkon 6LN- ja 6LR-laitteista. (7, s. 12–20.)

Reititys alkaa verkon isännän (6LBR) lähettämillä viesteillä. Laitteet, jotka ovat verkon isännän, alueella kuuntelevat näitä viestejä ja määrittelevät sen arvojen (DODAG-arvot) perusteella, liittyvätkö ne kyseisen isäntälaitteen verkkoon. Kun laite on liittynyt verkkoon, sillä on reitti kohti verkon isäntää. (7, s. 12–20.)

Verkkoon liittynyt laite määrittää verkon reitittimen isännäkseen ja laite määrittää oman sijansa (Rank) isäntää kohti. Mikäli verkkoon liittynyt laite toimii reitittimenä (6LR), se alkaa lähettää verkon tietoja (DODAG-arvot) sen alueella sijaitseville laitteille reittien luomiseksi. Verkon laitteet, jotka eivät toimi verkon reitittiminä, liittyvät verkkoon lähettämättä reititysviestejä (7, s. 12–20.)

Verkon alueella olevat laitteet toistavat tätä prosessia, kunnes jokainen alueella oleva laite on määritellyt oman isännän, reitin isäntään, sijansa ja verkon tiedot. (7, s. 12–20.)

3.1.3 RPL:n turvaominaisuudet

Reititysprotokollaan on olemassa tietoturvamekanismeja, jotka perustuvat IP-paketin salaukseen. Reititykseen kohdistuvia uhkia ovat erityyppiset uudelleenohjaus-, palvelunesto- ja osoiteväärennöshyökkäykset. IPv6-paketin salauksella ei pystytä turvaamaan verkon sisältä tulevia hyökkäyksiä vastaan, vaan se tarjoaa suojan verkon ulkopuolelta tulevia hyökkäyksiä. (7, s. 16–17.

RPL tukee kolmea tietoturvamekanismia:

- Turvaamaton: RPL käyttää verkon muodostuksessa suojaamattomia viestejä. Suojaamattomuus ei kuitenkaan tarkoita, että verkon viestimistä ei olisi suojattu jollain muulla menetelmällä.
- Esiasennetut salausavaimet: RPL käyttää verkon muodostuksessa suojattuja viestejä. Verkon reitittimellä tai isännällä on oltava esiasennettu salausavain. Tarjoaa viestityksen luotettavuuden, eheyden ja autentikoinnin.
- Autentikoitu: RPL käyttää verkon muodostuksessa esiannettuja salausavaimia ja verkon laite voi liittyä tämän avulla vain isäntänä verkkoon. Laitteen liittyessä verkkoon vaaditaan toinen salausavain. (7, s. 89–90.)

3.1.4 RPL:n salaus

6LoWPAN-järjestelmän salausmekanismit perustuu AES-128- ja CCM - Cryptographic Block Ciphers -salausalgoritmeihin, joiden käyttö yhdessä mahdollistaa luotettavuus-, saatavuus- ja eheysvaatimusten saavuttamisen. Kaikkien protokollan lähettämien viestien MAC-osoite on salattu käyttämällä edellä mainittuja salausalgoritmeja sekä käyttämällä RSA- ja SHA-256-salausmenetelmiä paketin allekirjoittamisessa. (7, s. 89–90.)

3.1.5 Salausvaimen hallinnointiin liittyvät riskit

6LoWPAN-verkoissa haittakoodi voi sijaita haavoittuneessa laitteessa. Tämä aiheuttaa sen, että verkkoa luodessa salausavainten luotettava jakaminen on haasteellista. Sleep-tilassa olleiden laitteiden salausavaimet tulee jakaa uudelleen jokaisella laitteen aktivoitumiskerralla. Mikäli haavoittuvuus huomataan, joudutaan koko verkon salausavaimet mitätöimään ja korjaamaan haavoittuvuus, jonka jälkeen salausavaimet voidaan uusia. Tämä tarkoittaa sitä, että 6LoWPAN-verkon laitteiden tulisi olla uudelleenohjelmoitavissa mahdollisia lisäyksiä varten. (2, s. 17–18.)

3.1.6 6LoWPAN-reitityksen viestit

Verkon topologian muodostamiseen käytettävät viestit määritellään 6LoWPAN-protokollaan liittyvässä IETF:n dokumentissa RFC 6775. Näitä viestejä kutsutaan dokumentissa nimillä Router Discovery -viestit ja Neighbor Discovery -viestit. Lisäksi näiden termien alla on viestit router solicitation, router association, neighbor solicitation ja neighbor association. Näitä viestien termejä käytetään dokumentin 4 ja 5 otsikoiden alla käsiteltävissä asioissa.

Tarkemmat tiedot IPv6-verkkojen reitittämisestä voi löytää IETF:n dokumentista RFC 4861, RFC 5942 ja RFC 6980. (13, s. 3.)

3.2 Secure Neighbor Discovery -protokolla

SeND (Secure Neighbor Discovery) on IPv6-verkoille verkon luonnin yhteyteen määritelty tieturvalisäys, joka määritellään dokumentissa RFC 3971. Sen tarkoitus on turvata reitityksen RS/RA-viestit, Neighbor Discovery -mekanismin NS/NA-viestit, osoitteen määritys, osoitteen selvitys, Neighbor Unreachability Detection -mekanismi(DUD), Duplicate Address Detection -mekanismi (DAD) ja yhteyksien uudelleenohjauksen yhteydessä. Sen periaatteena ovat seuraavat:

- Reittiä etsivän laitteen on tiedettävä luotettava reititin yhteyden luomiseen.
- CGAta käytetään laitteen naapureiden etsimen yhteydessä ND-viestien omistajan todentamiseen.
- RSA-allekirjoitus on optio, jota käytetään kaikkien ND- ja RD-viestien todentamiseen.
- ND-protokollaan on lisätty kaksi uutta ominaisuutta, Nonce ja aikaleima, joiden avulla estetään toistoon perustuvia hyökkäyksiä.

RFC 3971 -standardia on päivitetty dokumenteissa RFC 6494, 6495 ja 6980. (5, s. 6–8.)

3.3 CoAP-protokolla

Constrained Application Protocol (CoAP) on 6LoWPAN-verkkojen heikko tehoisille laitteille suunniteltu sovellustason protokolla. CoAP käyttää tiedon turvaamiseen Datagram Transport Layer Security (DTLS) -protokollaa. CoAP-protokolla määrittelee neljä eri tietoturvatasoa:

- NoSec: DTLS-protokolla ei ole käytössä. Alampien tasojen tietoturvaprotokollien, kuten IPsec-tietoturvaprotokollan käyttö suositeltavaa sitä tarvittaessa.
- PreSharedKey: DTLS-protokolla käytössä. Laitteilla on esiasennettuja salausavaimia, jotka mahdollistavat yhteydet vain tiettyihin nodeihin. Saman salausavaimen omaavat tahot kuuluvat tiettyyn ryhmään, ei mahdollista laitteiden välistä yhteyttä.
- RawPublicKey: DTLS-protokolla käytössä ja laitteilla on asymmetrinen julkinen salausavain ilman sertifikiointia, joka on validoitu laitteen valmistuksen yhteydessä. Laitteen identiteetti muodostetaan käyttäen tätä avainta, jonka avulla voidaan kertoa laitteet joiden kanssa se voi kommunikoida.
- Certificate: DTLS-protokolla on käytössä ja laitteella on asymmetrinen salausavainpari ja sertifikaatti X.509 (RFC 5280). Laite yhdistyy järjestelmässä tiettyyn luotettuun laitteeseen. (8.)

NoSec-tilassa protokollaa hyödyntävä laite lähettää paketit normaalisti käyttäen UDP:tä. CoAP-protokollaa hyödyntävä laite voi estää tällöin vain pakettien lähettämisen ja vastaanottamisen verkon laitteilta hyökkäyksen yhteydessä. (8.)

3.4 6LoWPAN: IEEE 802.15.4 MAC ja PHY

6LoWPAN-verkoissa protokollapinon IEEE 802.15.4 MAC-kerrosta käytetään verkon reitittämisessä. Reitittämiseen liittyvät tietoturvariskit ovat yksi verkon kriittisimmistä pisteistä ja vaativat vahvan tietoturvan. Reitityksessä tapahtuvaan IPv6-paketin fragmentointiin ja uudelleenkokoamiseen liittyy haavoittuvuuksia. Hyökkäyksiä voidaan toteuttaa muuntamalla paketin ominaisuuksia. Tunnettuja

hyökkäyksiä ovat Tiny Fragmentation, Ping of Death ja Jolt. Kyseiset hyökkäykset voivat aiheuttaa vakavia ongelmia laitteessa. (1.)

IPv6-standardin pakettikoko on 1280 oktettia. 6LoWPAN-järjestelmien fragmentaatio ja kokoamistoiminto mahdollistavat näiden pakettien käytön IEEE 802.15.4 -järjestelmissä. Hyökkäyksissä järjestelmiä kohtaan on käytetty hyväksi tätä paketin muokkausmenetelmää erilaisiin palvelunesto- ja toistohyökkäyksiin. Hyökkäys perustuu IPv6-paketin ominaisuuksiin: datagram size, datagram tag ja datagram offset. Näiden ominaisuuksien haitallinen muokkaaminen aiheuttaa järjestelmän laitteiden ylikuormitusta, joka voi johtaa järjestelmän jumiutumiseen tai uudelleenkäynnistymiseen. (10, s. 6–8; 12.)

4 6LOWPAN-REITITYKSEN TIETOTURVARISKIT

Suuri osa 6LoWPANia koskevista hyökkäyksistä voivat olla erittäin tuhovoimaisia. Verkon luonteen takia 6LoWPAN-laitteet ovat erittäin alttiita fyysisille hyökkäyksille, jolloin tuhot ovat pysyviä. Fyysisissä hyökkäyksissä laiteita kohtaan tulee huomioida myös laitteiden ohjelmiston ja elektronisten osien muutokset. Haittakoodin sijoittaminen yhteen laitteeseen voi vahingoittaa kaikkia sensoriverkon osia. Laitteen hallinnan menettäminen voi johtaa myös salauksessa käytettävien avainten menettämisen. (1.)

6LoWPANin valitun protokollan tyylin takia tulee verkkoon liittyviä uhkia arvioida jokaisella protokollapinon tasolla erikseen. Protokollapinon fyysisellä-tasolla eli sensoriverkon radioita vastaan voidaan toteuttaa useita erityyppisiä palvelunestohyökkäyksiä, salakuuntelua ja sähkömagneettiseen säteilyyn perustuvaa häirintää. Verkkokerroksella hyökkäys voi olla tahallinen tai tahaton MAC-osoitteeseen pohjautuva hyökkäys tai haitallisesti muokattujen TCP/IP-pakettien lähettäminen laitteisiin. Hyökkäysten voimaa tehostaa 6LoWPAN-laitteiden vähäiset resurssit. (1.)

4.1 Järjestelmän salakuuntelu

6LoWPAN-verkon luonnin yhteydessä laitteet ovat haavoittuvaisia salakuuntelulle. Kohteena voi olla järjestelmän salausavain, turvallisuusparametrit tai laitteen asetukset. Hyökkääjä voi näiden avulla purkaa järjestelmän salauksen jolloin tiedon salakuuntelu on mahdollista. (11, s. 5–9.)

4.2 Laitteiden jäljentäminen ja heikentäminen

Laitteiden valmistuksen yhteydessä tulee huomioida voidaanko laite kopioida tai tahallisesti heikentää haittamielessä. Tällaisissa tapauksissa haittalaite tai hyökkääjä voi käyttää hyödyksi saamiaan tietoja järjestelmän rakenteesta. Tämä mahdollistaa haittalaitteen toimimisen normaalisti verkossa ja mahdolliset takaovien asentamisen laitteisiin. (11, s. 5–9.)

4.3 Sybil -hyökkäykset

Sybil-hyökkäykset ovat hyökkäyksiä, joissa virheellinen, haavoittunut tai verkon ulkopuolinen laite käyttää useita erilaisia identiteettejä haitatakseen verkon toimintaa (5).

Sybil-hyökkäyksiä 6LoWPAN-verkkoja kohtaan voidaan kohdistaa verkon eri osiin. Kohteina voivat olla verkon tietokannat, reititysmekanismi, tiedon keräysmekanismit sekä erityyppiset verkon resursseja säätävät mekanismit. Tämän tyyppisiä hyökkäyksiä on erittäin vaikea havaita ja estää. (4.)

4.4 Black Hole -hyökkäykset

Black Hole -hyökkäykset ovat yksi palvelunestohyökkäyksien tyypeistä. Hyökkäyksessä reititin tai jokin verkon laitteista odottaa vastausta jostain verkon kohteesta, mutta ei sitä saa haittakoodilla saastutetun laitteen takia. Hyökkäys voi aiheuttaa myös kaiken verkossa kulkevan tiedon päätymisen saastuneelle laitteelle. (3.)

Hyökkäys perustuu siihen, että haittakoodilla saastutettu laite vastaa jokaiseen verkon kutsuun ja vastaa niihin väittämällä olevansa optimaalisin reitti haluttuun kohteeseen. Hyökkäys voi vaikuttaa laajalle verkkoon. (4.)

4.5 Wormhole-hyökkäykset

Wormhole-hyökkäyksessä nauhoitetaan lähetetyt paketit tai bitit jossain verkon kohteessa, jonka jälkeen tiedot tunneloidaan haluttuun kohteeseen. Hyökkäys ei vaadi haavoittunutta 6LoWPAN-laitetta ja se voidaan suorittaa jo verkon muodostus vaiheessa. (4.)

4.6 Rank-hyökkäys

Rank-hyökkäys hyödyntää reitittämisprotokollan sääntöä, jonka mukaan 6LN-laitteen sijaluku kasvaa, mitä kauempana laite on reitittimestä dataa vastaanotettaessa, ja laskee, mitä lähempänä laite on reititintä dataa lähetettäessä. Tämä sääntö estää laitetta tekemästä optimoimattomia reittejä tai

silmukkaa verkossa. Mikäli sääntö ei täyty tietoden välityksessä, tulee sen hetkisen laitteen asettaa Rank-Error-bitti RPL Packet Information -kenttään. (1.)

Sääntö ei kuitenkaan suojaa verkon sisältä tulevalta hyökkäykseltä. Hyökkäyksessä haavoittunut laite jättää tekemättä sijaluvun tarkistustoiminnon tai liikenteeseen lisätään haittakoodia, joka estää koko mekanismin. Aiheutunut haitta voi olla reitti jota ei ole optimoitu, yhteyksiä laitteisiin ei muodostu tai silmukka reitissä. (1.)

4.7 Local Repair -hyökkäys

6LoWPANille suunniteltu reititys (RPL) on haavoittuvainen niin kutsutulle Local Repair -hyökkäykselle, joissa saastunut laite ilmoittaa olevansa aktiivinen verkon laite ja lähettää oman sijatietonsa muille laitteille, sen jälkeen naapurina toimivat laitteet joutuvat etsimään uuden reitin isäntää kohti. (1.)

Hyökkäyksen voi toteuttaa myös muuttamalla laitteen DODAGID:n arvoa. DODAGID:n arvon muutos verkossa tarkoittaa, että laite on poistunut verkosta ja muut verkon laitteet joutuvat etsimään uuden reitin kohteeseensa. Verkon rikkoutuminen johtaa siihen, että kaikki likiverkon laitteet joutuvat suorittamaan Local Repair -mekanismin aina, kun hyökkäystä suorittava laite muuttaa DODAGID:n arvoa. (1.)

Hyökkäys on erittäin rasittava paikallista verkkoa kohti laitteiden vähäisten resurssien takia. Hyökkäys voi kuormittaa samalla useampaa erillistä likiverkkoa. (1.)

5 6LOWPAN-REITITTIMIEN RISKIT

6LoWPAN-järjestelmän reitittimenä toimivat laitteet käyttävät NDP:tä (Neighbor Discovery Protocol) löytääkseen likiverkon muut reitittimet ja määrittääkseen niiden verkkotason osoitteet reitittämistä varten. Mikäli NDP:tä ei ole suojattu, on järjestelmä haavoittuvainen reitittämisen yhteydessä. Seuraavat ongelmat koskettavat myös järjestelmän protokollapinon tasoja 6LoWPAN, IEEE 802.15.4 MAC ja IEEE 802.15.4 PHY. (4.)

5.1 Osoiteväärennös

Osoiteväärennökset ovat MAC-osoitteiden väärinkäyttämistä haitallisesti tai vahingossa. Laitteen uniikin MAC-osoitteen muodostamiseen käytettävä mekanismi mahdollistaa laitteelle määritellyn osoitteen väärentämisen, jolloin saman MAC-osoitteen esittävä haittalaite voi estää varsinaisen laitteen liittymisen verkkoon. Tällä voidaan tehdä niin kutsuttu uudelleenohjaus tai palvelunesto hyökkäys. (4, s. 9–10.)

Verkossa olevat laitteet käyttävät keskinäisten linkkien muodostamiseen NS- ja NA-viestejä. Hyökkäävä laite voi aiheuttaa verkon laitteille lähettyjen pakettien päätymisen väärään osoitekerroksen osoitteeseen. Hyökkäys onnistuu muokkaamalla NS-viestien lähteen osoiteosaa tai lähettämällä NA-viestin väärennetyllä osoitteella. Hyökkäys aiheuttaa laitteen osoitemuistin korvaamisen uudella osoitteella, koska uusi osoitetieto kirjoitetaan vanhan osoitteen päälle. Hyökkäys toimii niin kauan kuin hyökkäävä laite vastaa NS-viestiin väärennetyllä NA-viestillä. (4, s. 9–10.)

Järjestelmän tapaa, jolla osoite määritetään, voidaan hyödyntää järjestelmiä vastaan tehtävissä palvelunestohyökkäyksissä. Hyökkäys toteutetaan lähettämällä väärennetty käyttämätön osoite. Hyökkäyksen kesto voi olla lyhyt, jollei hyökkäävä laite pysty pitämään huijausta yllä, sillä NUD-mekanismi voi poistaa väärän osoitteen laitteen muistista ja lähettää uuden viestin oikean osoitteen löytämiseksi. NUD-mekanismia käytetään ylempien kerrosten liikenteessä liian pitkän viiveen esiintyessä tai kun laite ei pysty vastaanottamaan toisten laitteiden viestejä. NUD-mekanismi viestissä laitteet lähettää

kohdennetun NS-viestin toiselle laitteelle, joka vastaa NA-viestillä. NUD-mekanismi voi kuitenkin epäonnistua, jolloin laite käynnistää normaalin osoitteenselvitysprosessin uuden MAC-osoitteen selvittämiseksi. Mikäli NA-viestejä ei ole suojattu, voi hyökkäävä laite jatkaa väärennettyjen NA-viestien lähettämistä verkossa. (4, s. 9–10.)

Verkoissa, joissa siihen liittyvät laitteet käyttävät IP-osoitteen hakemiseen tilatonta autokonfiguraatiota, voi hyökkäävä laite käynnistää palvelunestohyökkäyksen vastaamalla jokaiseen isäntälaitteen lähettämään DAD-viestiin. Mikäli hyökkäävä laite onnistuu varaamaan osoitteen, oikea laite ei pysty ikinä selvittämään oikeaa osoitetta. Hyökkäys onnistuu kahdella eri tavalla: vastaamalla NS-viestillä, millä se simuloi tekevänsä DAD-mekanismia tai vastaamalla NA-viestillä, millä se simuloi varauksen haluttuun osoitteeseen. (4, s. 9–10.)

Kyseiset hyökkäykset voivat aiheuttaa tietoturvaongelmia 6loWPAN-verkoissa, vaikka verkkoon olisi määritelty luotettavat laitteet, mikäli yksi verkon laitteista on haavoittuvainen tälle hyökkäykselle. Tapauksissa, joissa vain verkon operaattori on määritelty luotettavaksi, muut laitteet voivat luottaa verkonhaltijan oikeaksi määrittelemiin osoitteisiin. Ad hoc-verkoissa laitteet voivat käyttää niin kutsuttua CGA-sertifiointitekniikkaa oikeiden linkkien löytämiseen tai kirjata yhteysvirheet ylös ja estämää ND-viestien hyväksymisen, ennen kuin laitteen muistissa oleva vanha osoite ei enää vastaa. (4, s. 9–10.)

5.2 Reitityshyökkäykset

Reitityshyökkäykset luokitellaan uudelleenohjaus- ja palvelunesto-hyökkäyksiksi. Nämä hyökkäykset ovat yleinen uhka IPv6-mobiiliverkoissa. (4, s. 12.)

Aliverkoissa, joissa isäntä laite yrittää löytää oikeaa reititintä, voi hyökkäävä laite huijata verkkoa lähettämällä väärän RA-viestin tai vastaamalla RA-viestillä oikean laitteen kyselyihin. Mikäli laite hyväksyy hyökkäävän laitteen, kaikki verkossa kulkeva liikenne siirtyy kulkemaan haittalaitteen lävitse. Tämä aiheuttaa sen, että haittalaite voi estää tiedon kulkemisen järjestelmän läpi kokonaan tai

osittain ja pystyy mahdollisesti tallentamaan kaiken reitittämänsä liikenteen. (4, s. 12.)

Hyökkäävä laite suojautuu lähettämällä jatkuvasti väärennettyjä RA-viestejä oikealle reitittimelle. Tämä perustuu siihen, että verkkoon liittyvät laitteet eivät voi saada varsinaiseen reitittimeen yhteyttä, koska hyökkäävä laite estää oikean reitittimen toiminnan omilla RA-viesteillään. Mikäli hyökkäävä laite onnistuu huijauksessa, siirtyvät kaikki verkkoon liittyvät laitteet sen alaisuuteen, luullen sitä oikeaksi reitittimeksi, koska oikea reititin ei vastaa niiden kutsuihin. Hyökkäyksen onnistuessa haittalaite voi lähettää uudelleenohjaus-iestin sen alaisuudessa oleviin laitteisiin ja kadota verkosta. (4, s. 12.)

Tämän tyyppisten uhkien mahdollisuutta voi rajoittaa vaatimalla, että RA-viestien osoitekentän prefix-osan elinikä on alle 2 tuntia ja vähemmän kuin tallennettu elinikä. Laitteiden asetukset voidaan säätää siten, että se suosii jo olemassa olevia reitittimiä uusien sijasta. Laitteiden säätäminen käyttämään jo olemassa olevia reitittimiä ei kuitenkaan estä täysin haittalaiteen liittymistä verkkoon. (4, s. 12.)

5.3 Reitittimen tuhoaminen

Hyökkäys jossa verkon reititin tuhotaan johtaa siihen, että verkossa olevat laitteet olettavat kaikkien laitteiden olevan paikallisia. Hyökkäys perustuu siihen, että hyökkäävä laite saa muut laitteet uskomaan reititystaulun olevan tyhjä. Reititystaulun ollessa tyhjä laitteet alkavat käyttää ND-mekanismia, ja tämä johtaa taas siihen, että hyökkäävä laite pystyy käyttämään NS/NA-viesti huijausta. (4, s. 13.)

Hyökkäys voidaan toteuttaa kahdella eri tavalla: palvelunestohyökkäyksellä tai väärennetyillä RA-viesteillä. Hyökkäys voidaan toteuttaa myös reitittimen ylikuormittamisella tai fyysisesti tuhoamalla reititin, jolloin verkossa ei tarvitse käyttää hyväkseen mahdollisia ND-mekanismin haavoittuvuuksia. Pääasiassa hyökkäys on palvelunestohyökkäys, mutta se mahdollistaa myös sen, että kaikki liikenne kulkee haittalaitteen lävitse. (4, s. 13.)

5.4 Väärennetty Redirect-viesti

Redirect-viestiä voidaan käyttää lähettämään paketteja haluttuun osoitteeseen verkon sisällä. Hyökkääjä käyttää verkon ensimmäisen reitittimen osoitetta lähettääkseen Redirect-viestin haluttuun kohteeseen. Kohde hyväksyy Redirect-viestin, koska viesti näyttää tulevan tunnetusta reitittimestä. Mikäli hyökkääjä onnistuu vastaamaan DUD-kyselyihin, Redirect-hyökkäys pysyy voimassa. (4, s. 14.)

Järjestelmässä voidaan käyttää luotettujen laitteiden listausta. Sitä käytettäessä tämäntyyppinen hyökkäys ei ole tehokas. Mikäli luotettu laite haavoittuu, tulisi muiden laitteiden osata tulkita verkko-operaattorin tai luotettujen laitteiden ero. Ad hoc -reitityksessä tämäntyyppiseen hyökkäykseen ei ole vastakeinoja. (4, s. 14.)

5.5 Väärennetty osoitekenttä

Hyökkäyksessä laite lähettää RA-viestin, jossa on mielivaltaisesti määritelty verkko-osoitteen prefix-osa. Viestin vastaanottava laite voi luulla osoitteen prefix-osan olevan verkossa ja tämä johtaa siihen, että laite ei lähetä datapakettia kyseiselle väärennettyä prefix-osaa omaavalle reitittimelle, vaan yrittää selvittää osoitetta NS-viestillä. NS-viesteihin ei kuitenkaan saada vastausta ja laitteen toiminta estyy, kunnes väärennetyn prefix-osion elinikä on nolla tai laite käynnistetään uudelleen. Hyökkäys voidaan toteuttaa myös kohdistetusti haluttuun osoitteeseen käyttämällä kohteen täydellistä osoitetta. (4, s. 14.)

Hyökkäys voi aiheuttaa palveluestohyökkäyksen kuormittamalla laitteen rajallisen reititystaulun. Kohteena oleva laite ei osaa erotella väärennettyjä ja oikeita osoitteen prefix-osia, jolloin laite ei osaa enää lähettää paketteja oikeisiin osoitteisiin. Hyökkäystä voidaan käyttää myös uudelleenohjaushyökkäykseen vastaamalla NS-viesteihin väärennetyllä NA-viestillä, jolloin verkossa olevat laitteet saadaan lähettämään paketit haluttuun osoitteeseen. (4, s. 14.)

Hyökkäys on erittäin helppo toteuttaa, mikäli yksi linkin laitteista on haavoittunut tai RA-viestien prefix-osion pituutta ei ole rajoitettu. (4, s. 14.)

5.6 Väärennetty aliverkko-osoite

Hyökkäävä laite voi käyttää RA-viesteissä väärää aliverkko-osoitteen prefix-osaa, jota käytetään normaalisti osoitteiden automaattiseen konfigurointiin. Hyökkäyksen kohteena oleva laite käyttää RA-viestissä lähetettyä prefix-osaa osoitteenmuodostus-algoritmissaan, vaikka prefix-osa on väärennetty. Tämä johtaa siihen, että NS-viestit eivät ikinä saa vastausta väärän osoitteen takia. (4, s. 15.)

Hyökkäys voi mahdollisesti levitä verkossa oleviin muihin kohteisiin, mikäli hyökkäyksen kohteena ollut laite suorittaa nimipalvelujärjestelmän päivityksen väärennetyllä osoitteella. Päivitys aiheuttaa väärennetyn osoitteen päätymisen osoitetauluun. Tämä johtaa siihen, että järjestelmät, jotka suorittavat osoitteen selvitystä järjestelmän avulla, saavat väärennetyn osoitteen, johon ei voi saada yhteyttä. Hyvin toteutettu järjestelmän ohjelmisto osaa kuitenkin kiertää hyökkäyksen tarkastamalla laitteen DNS-osoitetaulun ja vertaamalla sitä laitteisiin kyselyihin. (4, s. 15.)

5.7 RA-viestin parametrien väärentäminen

RA-viestit sisältävät parametreja, joita käytetään IPv6-osoitteen tilallisessa osoitteenmuodostuksessa laitteissa. Hyökkäävä laite voi lähettää oikealta näyttävän RA-viestin, joka on jäljennös oikeasta RA-viestistä, mutta jonka parametrien arvoja on muutettu haitallisesti. Hyökkäyksen tarkoitus on estää järjestelmän palvelut. Tyypillisesti hyökkäys toteutetaan muuttamalla parametrin Current Hop Limit-lukua joko arvoksi 1 tai joksikin pieneksi luvuksi. Tämä aiheuttaa pakettien putoamisen. Lisäksi hyökkääjä voi luoda väärennetyn DHCPv6-palvelun tai toistimen, jossa määritellään tuleeko kohteen suorittaa tilallinen tai tilaton osoitteenmuodostus, jolloin hyökkääjä voi vastata osoitteenmuodostuskyselyihin omilla väärennetyillä vastauksilla. (4, s. 16.)

DHCP-palvelun turvaaminen ei poista ongelmaa, sillä hyökkäys voidaan toteuttaa paikallisesti, jolloin laite ei pääse suorittamaan osoitteenmuodostus kyselyä tai se saa laitteen käyttämään väärää DHCP-palvelua. Hyökkäyksen

tehoa voidaan minimoida asettamalla järjestelmän Hop Limit-laskurin minimiarvon estämään pienet arvot. (4, s. 16.)

5.8 Replay-hyökkäykset

Kaikkia reitittämiseen liittyviä viestejä uhkaa niin kutsutut toistohyökkäykset. Toistohyökkäys voidaan toteuttaa, vaikka viesti olisi salattu, koska hyökkäyksessä käytetään oikeita viestejä, joita toistetaan hyökkäyksen aikana. (4, s.18.)

5.9 Neighbor Discovery -palvelunestohyökkäys

Neighbor Discovery -palvelunestohyökkäysessä laite aloittaa toistuvan viestien lähettämisen, jossa aliverkon osoitteen prefix-osa on väärennetty. Verkon viimeisen reitittimen osoitteenselvitys-tekniikka pakottaa reitittimen lähettämään NS-viestejä, jolloin muut verkon laitteet eivät saa siltä ND-palveluita. Hyökkääjän ei tarvitse olla paikallisessa verkossa. (4, s. 18.)

6 TIETOTURVAN SUUNNITTELU

6LoWPAN-järjestelmät usein vaativat jonkinlaisen tietoturvasuunnitelman takaamaan, että siirrettävä tieto on luotettavaa ja siirretty tieto pysyy eheänä. Tietoturvamekanismin voi luoda esimerkiksi protokollapinon sovellus, verkko tai siirtokerrokseen. Tietoturvasuunnitelmassa 6LoWPAN-järjestelmälle tulee huomioida niiden pieni ohjelmistomuistin koko, matala tehoisuus, yksinkertaisuus ja kaistanleveys. Lisäksi pitää arvioida, kuinka erilaiset haavoittuvuudet ja palvelunestohyökkäykset vaikuttavat suunniteltavaan järjestelmään. 6LoWPAN-järjestelmän vähäisten resurssien takia on tärkeää arvioida, millaisella tavalla tietoturvamekanismi tulisi toteuttaa itse laitteistossa ja vaatiiko se rinnalleen erillisen tietoturvamekanismin. (9.)

6LoWPAN-järjestelmien vaatimukset on määritelty RFC4919 dokumentissa. Sen pääperiaatteita ovat seuraavat:

- Luotettavuus: vain luotetut laitteet voivat tarkastella tietoja.
- Todennus: tieto voidaan hyväksyä vain luotettavista lähteistä.
- Eheys: siirretty tieto pysyy muuttumattomana lähetyksen aikana.
- Tuoreus: tietoa ja salausavaimia ei pystytä uudelleen käyttämään.
- Saatavuus: tieto on helposti saatavilla kun sitä tarvitaan.
- Kestävyys: järjestelmän on toimittava epänormaaleissa tilanteissa ja tilanteissa, missä yksi järjestelmän osista on haavoittunut.
- Tehokkuus: Tietoturvajärjestelmän ei tulisi viedä paljon resursseja.
- Takuu: Järjestelmän on taattava, että se pystyy erottelemaan tulevan tiedon.

Korkeiden tietoturvaperiaatteiden saavuttamiseksi 6LoWPAN-järjestelmät voivat vaatia rinnalle mahdollisia muita tietoturvajärjestelmiä, sillä salaus voi taata vain järjestelmän tiedon luotettavuuden, todennuksen ja eheyden.(1; 2, s. 9–10; 9, s. 2–3.)

6.1 Tietoturvaohjeet

IETF:n dokumentissa RFC 6568 on tutkittu erilaisten käyttökohteiden mahdollisuutta ja niiden tietoturva vaatimuksia. Määrittelyt ovat suuntaa antavia ohjeita 6LoWPAN-järjestelmien kehittäjille.

- Teollisuusjärjestelmien tietoturva: Kriittinen, salattu tietoliikenne tulee taata, haavoittuvuudet vakavia liiketoimelle.
- Rakennusjärjestelmien tietoturva: Turvallisuus-kriittinen, salattu liikenne tulee taata ja vain tunnistetut käyttäjät ja laitteet hyväksytään tiedon käsittelyyn.
- Kotijärjestelmien tietoturva: Autentikaatio ja salaus vaadittavaa.
- Terveydenhoitojärjestelmien tietoturva: Datan yksityisyys ja turvallisuus on taattava. Salaus vaadittavaa. Tieto on avoinna vain hyväksytyille käyttäjille.
- Auto ja liikennejärjestelmien tietoturva: Fyysisten vaurioiden ja tiedonsiirron heikkouksien hallinta tulee suunnitella.
- Maatalousjärjestelmien tietoturva: Riippuu käyttökohteesta, kevyt tietoturvataso ja salaus. (8, s. 8–24.)

RFC 6568 painottaa tämän lisäksi kiinnittämään huomiota dokumentteihin RFC 4919, RFC 6282 ja RFC 6775 sekä niissä mainittuihin tietoturvariskeihin järjestelmien suunnitellussa. (8, s. 8–24.)

6.2 Tunkeilijan havaitsemisjärjestelmät

Perinteisten tunkeilijan havaitsemisjärjestelmien eli IDS-järjestelmien tarkoituksena on tarkkailla verkossa liikkuvaa dataa ja pyrkiä havaitsemaan mahdolliset hyökkäykset verkkoon. IP-verkoille suunniteltuja IDS-järjestelmiä voi hyödyntää 6LoWPAN-verkon reitittimen ja Internetin välisessä liikenteessä. Ne eivät kuitenkaan sovellu hyvin 802.15.4- ja 6LoWPAN-pohjaisten langattomien

verkkojen tarkkailuun suurien resurssivaatimuksien ja niihin kohdistuvien hyökkäysten tyypin takia. (1.)

Tietoliikenteen poikkeusten seurantaan pohjautuvat IDS-järjestelmät soveltuvat 6LoWPAN-järjestelmän tietoliikenteen seurantaan hyvin, sillä ne eivät vaadi valtavasti resursseja hyökkäysten selvityksessä. Ongelmana on kuitenkin tämäntyyppisten järjestelmien aiheettomien hälytysten ja normaalin virhetilanteiden erottelukyky. (1.)

7 YHTEENVETO

Opinnäytetyön tarkoituksena oli tutkia 6LoWPAN-järjestelmien tietoturvaa, sekä kirjoittaa dokumentti, jonka avulla lukija voi tutusta 6LoWPAN-järjestelmien tietoturvamekanismeihin, riskeihin ja tietoturvasuunnitteluun. Tutkimuksen perusteena toimivat IETF:n 6LoWPAN:ia käsittelevät standardit, sekä erilaiset tietoturvaa käsittelevät tutkimukset. Lähteiden perusteella laadittiin tämä aihetta käsittelevä dokumentti.

Tutkimuksen tekijä oppi IPv6-pohjaisten likiverkkojen tietoturvasta kattavasti ja loppuraportin kokonaisuudesta tuli kattava katsaus 6LoWPAN-järjestelmien tietoturvamekanismeihin ja niihin liittyviin riskeihin. Opinnäytetyön loppuraportin kirjoittamisessa oli vaikeuksia, jonka takia työ myöhästyi aikataulusta. Nämä kirjoittamiseen liittyvät ongelmat saatiin kuitenkin ratkaistua.

6LoWPAN-standardeihin pohjautuvat järjestelmät käyttävät tehokkaita tietoturvamekaniikoita tiedonsiirron turvaamiseksi. Salausjärjestelmät takaavat kuitenkin vain tietoturvan luotettavuuden, eheyden ja saatavuuden. Jokaisen 6LoWPAN-järjestelmän tietoturva tulee suunnitella tarkasti huomioiden tietoturvaohjeet ja varmistamalla, että käytössä olevat laitteet eivät haavoitu.

LÄHDELUETTELO

1. Le, Anthtuan – Loo, Jonathan – Lasebae, Aboubaker – Aiash, Mahdi – Luo, Yuan, 2012. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. International Journal of Communication Systems Vol 25, nro 9, S. 1189–1212. Saatavissa: http://onlinelibrary.wiley.com/doi/10.1002/dac.2356/abstract. Hakupäivä 11.11.2013.

2. Park, S. – Kim, K. – Haddad, W. – Chakrabarti, S. – Laganier. J., 2011. IPv6 Over Low Power WPAN Security Analysis. The Internet Engineering Task Force (IETF). Saatavissa: http://tools.ietf.org/html/draft-daniel-6lowpan-security-analysis-05. Hakupäivä 11.11.2013.

3. Montenegro, G. – Kushalnagar, N. – Hui, J. – Culler, D, 2007. RFC 4944 Transmission of IPv6 Packets over IEEE 802.15.4. The Internet Engineering Task Force (IETF). Saatavissa: http://tools.ietf.org/html/rfc4944. Hakupäivä 11.11.2013.

4. Nikander, P. – Kempf,J. – Nordmark, E., 2004. RFC 3756 IPV6 Neighbor Discovery (ND) Trust models and threats. The Internet Engineering Task Force (IETF). Saatavissa: http://www.ietf.org/rfc/rfc3756.txt. Hakupäivä 11.11.2013.

5. Douceur, John R., 2002. The Sybil Attack. Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS). Saatavissa: http://www.few.vu.nl/~mconti/teaching/ATCNS2010/ATCS/Sybil/Sybil.pdf. Hakupäivä 11.11.2013.

6. Arkko, Jari – Kempf, J. – Zill, B. – Nikander, P., 2005. RFC 3971 SEcure Neighbor Discovery (SEND). The Internet Engineering Task Force (IETF). Saatavissa: http://www.ietf.org/rfc/rfc3971.txt. Hakupäivä 11.11.2013

7. Winter, T – Thubert, P. – Brandt, A. – Hui, J. – Kelsey, R. – Levis, P. – Pister, K. – Struik, R. – Vasseur, JP. – Alexander, R., 2012. RFC 6550 RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. The Internet Engineering

Task Force (IETF). Saatavissa: http://tools.ietf.org/html/rfc6550. Hakupäivä 11.11.2013.

8. Shelby, Z. – Hartke, K. – Bormann, C., 2013. Constrained Application Protocol (CoAP). The Internet Engineering Task Force (IETF). Saatavissa: http://tools.ietf.org/html/draft-ietf-core-coap-18. Hakupäivä 11.11.2013.

9. Kim, E. – Kaspar, D. – Vasseur, JP., 2012. RFC 6568 Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). The Internet Engineering Task Force (IETF). Saatavissa: http://tools.ietf.org/html/rfc6568. Hakupäivä 11.11.2013.

10. Kushalnagar, N. – Montenegro, G. – Schumacher, C., 2007. RFC 4919 IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. The Internet Engineering Task Force (IETF). Saatavissa: http://tools.ietf.org/html/rfc4919. Hakupäivä 11.11.2013.

11. Garcia-Morchon, O – Kumar, S. – Keoh, S. – Hummen, R. – Struik, R., 2013. Security considerations in the IP-based Internet of Things. The Internet Engineering Task Force (IETF). Saatavissa: http://tools.ietf.org/html/draft-garcia-core-security-06. Hakupäivä 20.11.2013.

12. HyonGon, Kim, 2008. Protection against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer. International Conference on Convergence and Hybrid Information Technology 2008, Daejeon, Etelä-Korea. Saatavissa: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4622925&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4622925. Hakupäivä 11.11.2013.

13. Shelby, Z. – Chakrabarti, S. – Nordmark, E. – Bormann, C., 2012. RFC 6775 Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). The Internet Engineering Task Force (IETF). Saatavissa: http://tools.ietf.org/html/rfc6775. Hakupäivä 28.11.2013